At the last cc meeting a request was made from a representative of SRPD for approval to dedicate a certain amount of funds (100K?) toward the acquisition of an LPR system. At that same meeting one of the council members ("having read the contract") noticed that there was some language in the contract related to the use of the information collected of concern. One of the responses from the vendor representative ("who appeared more salesman than either compliance, or technician") responded with a fuzzy answer like "the data is anonymized," and "servers are housed in the US" neither of which addressed the concern. Further questions exposed more reasons for concern on the use of the data: like what was really being collected, and who would have access to it. The determination was to approve the SRPD request BUT ALSO to review the contract to make sure that privacy was being protected. The city attorney accepted the latter as an action item. The latter would have an impact on the SRPD request depending on the finding.

Subsequent to the meeting an independent review of publicly available information led to some other finding related to LPR that were not known at the time of the above-mentioned meeting which might have some bearing in the determination of, if and how to use LPR in SR. For brevity we are using bullet points

- According to California law since 2015, Title 1.81.23 of the California Civil Code (Calif. Civil Code §§ 1798.29, 1798.90.5) regulates the use of automated license plate readers (ALPRs.)1. The law regulates the use of ALPRs by law enforcement agencies and requires them to have a privacy policy that includes specified information1.
    - Reinforces the importance and need for a privacy policy.
- ALPR Policy (srpd.org) - https://www.srpd.org/alpr-policy - Has reference to this company: Vigilant Solutions is the custodian and owner of the ALPR system.
    - The question is if this is the company of record or are there two providers, and how do they relate.
- ALPR Policy (srpd.org) - mentions a privacy policy which may or not apply to FLOCK systems (the new or additional vendor)
    - Bringing in a second vendor creates data concerns different from the ones when there is a single vendor.
- Proposition 47 – While the residents are quite happy to hear that a system is being acquired to assist in the growing numbers of thief's in the county the result might be less effective due to this enactment.
- There was no mention, nor could I find any for a data security expert looking at the use of this information in context beyond a reference to a "compliance" person related to the Vigilant Solutions.
    - Compliance and Data security while related are not the same discipline. If there is a step in this process related to data security it was not made clear in any meeting to date.

At issue is how the data is stored, especially since the SRPD has access to many other data stores, and in the worst case if they were to house all the combined data from these very sensitive (from a privacy view) collections in a single server, designed to help identify and apprehend, that was then accessible by any vendor, or subject to search by any other government agency it creates much concern. AL